528,312

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. April 2004 (01.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/028076 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32

(21) Internationales Aktenzeichen: PCT/EP2003/010327

(22) Internationales Anmeldedatum:
17. September 2003 (17.09.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
02020818.7 17. September 2002 (17.09.2002) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

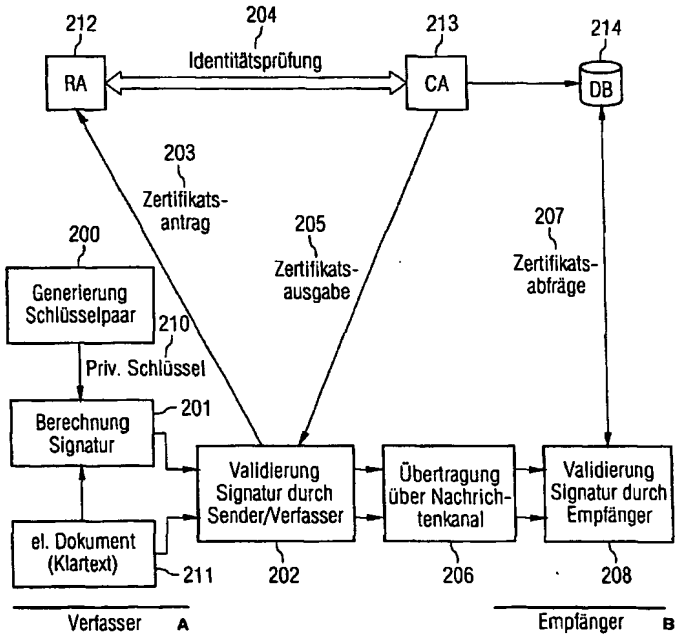
(75) Erfinder/Anmelder *(nur für US)*: **HEINTEL, Markus** [DE/DE]; Josef-Retzer-Str. 29, 81241 München (DE). **FURCH, Andreas** [DE/DE]; Moosstrasse 88, 85356 Freising (DE). **FRANKE, Markus** [DE/DE]; Gute Änger 26, 85356 Freising (DE). **PFAFF, Oliver** [DE/DE]; Grossgörschenstr. 5, 10827 Berlin (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GENERATING AND/OR VALIDATING ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUR ERZEUGUNG UND/ODER VALIDIERUNG ELEKTRONISCHER SIGNATUREN



200 GENERATION OF KEY PAIR
201 CALCULATION OF SIGNATURE
202 VALIDATION OF SIGNATURE BY SENDER/AUTHOR
203 CERTIFICATE REQUEST
204 VERIFICATION OF IDENTITY
205 ISSUE OF CERTIFICATE
206 TRANSMISSION VIA MESSAGE CHANNEL
207 CERTIFICATE INQUIRY
208 VALIDATION OF SIGNATURE BY RECIPIENT
210 PRIVATE KEY
211 ELECTRONIC DOCUMENT (PLAINTEXT)
A AUTHOR
B RECIPIENT

(57) Abstract: The invention relates to a method for generating and/or validating electronic signatures during which an asymmetric key pair is generated that comprises a private signature key and a public validation key. In addition, at least one electronic signature is calculated by using the private signature key and by applying a predeterminable signature function for at least one electronic document. A certification of the public validation key ensues after the calculation of the at least one electronic signature.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen, bei dem ein asymmetrisches Schlüsselpaar erzeugt wird, das einen privaten Signaturschlüssel und einen öffentlichen Validierungsschlüssel umfasst. Ausserdem wird zumindest eine elektronische Signatur mittels des privaten Signaturschlüssels und durch Anwendung einer vorgebbaren Signaturfunktion für zumindest ein elektronisches Dokument berechnet. Nach

[Fortsetzung auf der nächsten Seite]

WO 2004/028076 A1

(81) Bestimmungsstaaten *(national)*: CN, JP, KR, US.

Veröffentlicht:
— *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen

Elektronische Signaturen werden verwendet, um Sicherheitsziele wie Authentizität, Verbindlichkeit und Integrität zu erreichen. Falls elektronische Daten als Willenserklärung interpretiert werden können, dient ein positives Ergebnis einer Prüfung einer elektronischen Signatur als Beweismittel für deren rechtliche Wirksamkeit. Elektronische Signaturen arbeiten mit zwei Schlüsseln, die gemeinsam erstellt und mathematisch voneinander abhängig sind. Einer dieser Schlüssel - nachfolgend privater Schlüssel - wird geheimgehalten und kann zur Erstellung einer elektronischen Signatur verwendet werden. Der andere Schlüssel - nachfolgend öffentlicher Schlüssel - wird veröffentlicht und kann zur Verifikation einer geleisteten Signatur verwendet werden. Um elektronische Signaturen Personen zuzuordnen, bedarf es einer Bindung des Namens einer Person an den entsprechenden öffentlichen Schlüssel. Diese Bindung erfolgt in der Form eines speziellen elektronischen Dokumentes, welches von einer vertrauenswürdigen dritten Instanz ausgestellt und als Zertifikat bezeichnet wird.

Technisch gesehen sind Zertifikate Datenstrukturen, die Informationen enthalten, mit denen eine Bindung von öffentlichen Schlüsseln an Schlüsselinhaber gewährleistet wird. Die konkrete Bindung eines öffentlichen Schlüssels an einen bestimmten Schlüsselinhaber wird durch eine vertrauenswürdige und neutrale Zertifizierungsstelle (CA - certification authority) vorgenommen, die das zugehörige vollständige Zertifikat mit ihrer elektronischen Signatur beglaubigt. Zertifikate haben nur eine begrenzte Gültigkeitsdauer, die ebenfalls als Bestandteil des Zertifikates von der Zertifizierungsstelle mitsigniert ist.

Die Zertifizierungsstelle übernimmt die Prüfung des Namens und bindet durch eine elektronische Signatur (mit ihrem privaten Schlüssel) den Namen der Person an den öffentlichen Schlüssel dieser Person. Das Resultat der Zertifizierung eines öffentlichen Schlüssels ist ein Zertifikat. Als Zertifikatsstruktur wird der Standard X.509 benutzt. Solch ein Zertifikat umfaßt neben dem öffentlichen Schlüssel den Namen der ausstellenden Zertifizierungsstelle, einen Gültigkeitszeitraum, den Namen des Eigentümers und eine eindeutige Nummer der ausstellenden Zertifizierungsstelle. Hierbei wird vorausgesetzt, daß alle beteiligten Personen dem öffentlichen Schlüssel dieser Zertifizierungsstelle vertrauen. Zertifizierungsstellen besitzen getrennte Schlüsselpaare für das Signieren von Zertifikaten, Sperrlisten und Zeitstempeln sowie für die Abwicklung der Kommunikation mit anderen Kommunikationspartnern.

Bekannte Signaturverfahren bestehen aus einem Algorithmus zur Erzeugung elektronischer Signaturen und einem zugeordneten Algorithmus zur Verifikation elektronischer Signaturen. Die elektronischen Daten, für die eine elektronische Signatur gebildet wird, werden üblicherweise als Anhang den elektronisch signierten Daten beigefügt. Jeder Algorithmus zur Erzeugung elektronischer Signaturen erhält als Eingangsparameter zumindest zu signierende Daten sowie einen privaten Schlüssel eines Unterzeichners und liefert als Ergebnis eine elektronische Signatur. Der zugeordnete Algorithmus zur Verifikation elektronischer Signaturen erhält als Eingangsparameter zumindest elektronisch signierte Daten sowie einen öffentlichen Schlüssel eines Unterzeichners und liefert ein positives oder negatives Verifikationsergebnis, je nach dem, ob die Verifikation erfolgreich war.

Eine Erzeugung elektronischer Signaturen erfolgt bisher entsprechend nachstehender Reihenfolge:

- Erzeugung eines asymmetrischen Schlüsselpaars mit einem privaten und einem öffentlichen Schlüssel,

- Ausstellung eines Zertifikats für den öffentlichen Schlüssel,
- Bestimmung eines Hashwertes für die zu signierenden Daten,
- Berechnung der elektronischen Signatur durch Anwendung einer vorgegebenen Signaturfunktion,
- Ausgabe der elektronischen Signatur.

Eine Verifikation elektronischer Signaturen erfolgt bisher entsprechend nachstehender Reihenfolge:

- Bestimmung eines Hashwertes der elektronischen Daten aus dem Anhang zur elektronischen Signatur,
- Anwendung einer vorgegebenen Verifikationsfunktion auf die elektronische Signatur und den Hashwert,
- Ausgabe des Verifikationsergebnisses.

Signaturverfahren unterscheiden sich durch die verwendete Signatur- und Verifikationsfunktion (z.B. RSA, DSA oder ECDSA), einen verwendeten Hashalgorithmus zur Bestimmung des Hashwertes (z.B. SHA-1 oder RIPEMD-160) und ein ggf. verwendetes Paddingverfahren (bei RSA). Ein Paddingverfahren wird angewendet, um einen Hashwert durch eine vorgebbare Zeichenkette zu ergänzen, falls eine Anpassung der Länge des Hashwertes erforderlich ist.

Bisher bekannten Signaturverfahren ist ein hoher Aufwand zur dauerhaften Sicherung des privaten Signaturschlüssels auf Seiten der Person, welcher der private Signaturschlüssel zugeordnet ist, gegen unberechtigten Zugriff gemeinsam.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde ein Verfahren zur Erzeugung von elektronischen Signaturen zu schaffen, das keine dauerhafte Sicherung eines privaten Signaturschlüssels auf Seiten einer Person, welcher der private Signaturschlüssel zugeordnet ist, gegen unberechtigten Zugriff erfordert.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen des erfindungsgemäßen Verfahrens sind in den abhängigen Ansprüchen angegeben.

Ein wesentlicher Aspekt der vorliegenden Erfindung besteht darin, daß eine Zertifizierung eines öffentlichen Validierungsschlüssels erst nach einer Berechnung einer elektronischen Signatur erfolgt. Eine willentliche, durch ein signiertes Dokument ausgedrückte Handlung seitens eines Verfasser eines elektronischen Dokuments erfolgt somit erst nach Signaturgenerierung im Rahmen eines Zertifikatsbeantragungsprozesses. Da nicht eine Veranlassung einer Berechnung einer elektronischen Signatur, sondern eine Zertifikatsbeantragung die willentliche Handlung darstellt, ist es nicht erforderlich, einen zum öffentlichen Validierungsschlüssel korrespondierenden privaten Signaturschlüssel nach Berechnung der elektronischen Signatur aufzubewahren. Daher kann der private Signaturschlüssel nach Berechnung der elektronischen Signatur vernichtet werden und muß daher nicht mehr gegen unberechtigten Zugriff gesichert werden.

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt

Figur 1 eine Darstellung eines Ablaufs eines herkömmlichen Signaturverfahrens,

Figur 2 eine Darstellung eines Ablaufs eines erfindungsgemäßen Signaturverfahrens.

In Figur 1 ist ein Ablauf eines herkömmlichen Signaturverfahrens dargestellt, bei dem zunächst ein Schlüsselpaar generiert wird, das einen privaten Signaturschlüssel 110 und einen öffentlichen Validierungsschlüssel umfaßt (Schritt 100). Nachfolgend wird ein Zertifikatsantrag bei einer Registrierungsstelle 112 (RA - registration authority) gestellt

(Schritt 101). Im Zusammenspiel zwischen der Registrierungsstelle 112 und einer Zertifizierungsstelle 113 (CA - certification authority) wird eine Identitätsprüfung in Bezug auf einen jeweiligen Antragssteller vorgenommen (Schritt 102).

Bei einem positiven Überprüfungsergebnis vergibt die Zertifizierungsstelle 113 ein Zertifikat für den öffentlichen Validierungsschlüssel an einen jeweiligen Antragssteller (Schritt 103) und speichert einen entsprechenden Eintrag für das ausgegebene Zertifikat in einer der Zertifizierungsstelle 113 zugeordneten Datenbasis 114 ab, die zur Zertifikatsabfrage öffentlich zugänglich ist. Außerdem sind in der Datenbasis 114 Zertifikatssperrlisten gespeichert, die über ungültige Zertifikate informieren. Nach Zertifizierung des öffentlichen Validierungsschlüssels wird für ein zu signierendes elektronisches Dokument 111 eine elektronische Signatur unter Verwendung des privaten Signaturschlüssels 110 und einer vorgebbaren Signaturfunktion berechnet (Schritt 104). Anschließend werden die berechnete Signatur und das elektronische Dokument 111 über einen Nachrichtenkanal vom Verfasser des elektronischen Dokuments 111 als Nachricht an einen Empfänger des elektronischen Dokuments 111 übertragen (Schritt 105).

Empfängerseitig wird zur Validierung der elektronischen Signatur eine Zertifikatsabfrage noch vorgenommen (Schritt 106). Dabei wird entweder ein dem Verfasser zugeordneter öffentlicher Validierungsschlüssel aus der Datenbasis 114 abgefragt, oder es wird ein dem in der übertragenden Nachricht enthaltenen öffentlichen Validierungsschlüssel zugeordneter Eintrag in der Datenbasis 114 abgefragt, der ggf. die Gültigkeit des zugeordneten Zertifikats bestätigt. Abschließend wird eine Validierung der in der übertragenen Nachricht enthaltenen Signatur durch den Empfänger vorgenommen (Schritt 107). Bei der Validierung der elektronischen Signatur durch den Empfänger wird einerseits die Signatur mit Hilfe des öffentlichen Validierungsschlüssels entschlüsselt und andererseits ein Hash-Wert für das elektronische Dokument 111 berechnet. Ab-

schließend werden die entschlüsselte Signatur und der berechnete Hash-Wert auf Übereinstimmung verglichen. Bei Übereinstimmung der entschlüsselten Signatur und des berechneten Hash-Wertes wird die Signatur empfängerseitig als gültig anerkannt.

In Figur 2 ist ein Ablauf eines erfindungsgemäßen Signaturverfahrens dargestellt, bei dem zunächst ein asymmetrisches Schlüsselpaar erzeugt wird (Schritt 200). Mittels eines vom generierten Schlüsselpaar umfaßten privaten Signaturschlüssels 210 und einer vorgebbaren Signaturfunktion wird aus einem elektronischen Dokument 211 verfasserseitig eine elektronische Signatur berechnet (Schritt 201). Nach Berechnung der elektronischen Signatur wird diese durch den Verfasser validiert, um sicherzustellen, daß die berechnete elektronische Signatur einer durch das elektronische Dokument 111 ausgedrückten Willenshandlung entspricht (Schritt 202).

Bei einem positiven Validierungsergebnis wird ein Zertifikat für einen zum privaten Signaturschlüssel 210 korrespondierenden öffentlichen Validierungsschlüssel bei einer Registrierungsstelle 212 beantragt (Schritt 203). Nachfolgend werden im Zertifikatsantrag enthaltene Angaben überprüft, insbesondere die Identität des Verfassers bzw. eines Antragsstellers (Schritt 204).

Bei einem positiven Überprüfungsergebnis wird von einer Zertifizierungsstelle 213 ein Zertifikat für den öffentlichen Validierungsschlüssel an den Antragssteller bzw. Verfasser des elektronischen Dokuments 211 ausgegeben (Schritt 205). Außerdem wird ein entsprechender Eintrag in einer der Zertifizierungsstelle 213 zugeordneten Datenbasis für das ausgegebene Zertifikat vorgenommen.

Nach Validierung der berechneten Signatur durch den Verfasser des elektronischen Dokuments 211 und nach Zertifizierung des öffentlichen Validierungsschlüssels werden das elektronische

Dokument 211 und die berechnete elektronische Signatur als Nachricht zu einem Empfänger des elektronischen Dokuments 211 über einen Nachrichtenkanal übertragen (Schritt 206). Empfängerseitig wird in bekannter Weise eine Zertifikatsabfrage vorgenommen (Schritt 207) und eine Validierung der in der empfangenen Nachricht enthaltenen Signatur durchgeführt (Schritt 208).

Bei der Validierung einer elektronischen Signatur werden nur solche Signaturen als gültig anerkannt, die zu einem Zeitpunkt vor der Zertifizierung des öffentlichen Validierungsschlüssels erzeugt wurden. Hierdurch entfällt die bei bisherigen Signaturverfahren bekannte Revokationsproblematik in bezug auf öffentliche Validierungsschlüssel. Außerdem kann auf diese Weise nach dem Zeitpunkt der Zertifizierung des öffentlichen Validierungsschlüssels kein Mißbrauch mehr mit dem privaten Signaturschlüssel betrieben werden, so daß keine Mechanismen zur dauerhaften Vermeidung unberechtigter Zugriffe auf den privaten Signaturschlüssel 210 erforderlich sind.

Bei der Zertifizierung des öffentlichen Validierungsschlüssels entsprechend den Schritten 203 bis 205 kann zusätzlich zu einem Benutzeridentifikator und dem öffentlichen Validierungsschlüssel eine Referenz auf das jeweils signierte elektronische Dokument 211 einbezogen werden. Bei der empfängerseitigen Validierung der Signatur gemäß Schritt 208 wird dann die Referenz zum elektronischen Dokument 211 zusätzlich ausgewertet. Darüber hinaus ist es möglich, nicht nur eine Referenz auf ein einziges elektronisches Dokument in die Zertifizierung des öffentlichen Validierungsschlüssels einzubeziehen, sondern eine Mehrzahl von Referenzen auf innerhalb eines bestimmten Bezugszeitraumes signierte elektronische Dokumente. Eine Referenz auf ein elektronisches Dokument wird beispielsweise durch eine Berechnung eines Hash-Wertes für das jeweilige elektronische Dokument implementiert. Bei einer empfängerseitigen Validierung der Signatur entsprechend

Schritt 208 werden dann die entsprechenden Hash-Werte miteinander verglichen.

Eine Anwendung des erfindungsgemäßen Signaturverfahrens ist beispielsweise innerhalb eines zentralen Hardware-Sicherheitsmoduls möglich. Hierbei steht sämtlichen Mitgliedern einer geschlossenen Benutzergruppe ein privater Signaturschlüssel im zentralen Hardware-Sicherheitsmodul gemeinsam zur Verfügung. Benutzerseitig werden Hash-Werte für zu signierende elektronische Dokumente erzeugt und über einen geschützten Übertragungskanal an das Hardware-Sicherheitsmodul übermittelt. Das Hardware-Sicherheitsmodul berechnet ohne weitere Überprüfung die elektronische Signatur und sendet diese zurück einen jeweiligen Benutzer. Der jeweilige Benutzer speichert das signierte elektronische Dokument mit zugehörigem Hash-Wert und elektronischer Signatur nach erfolgreicher Validierung der Signatur durch den jeweiligen Benutzer ab. Die zugehörigen Hash-Werte werden zu einem späteren Zeitpunkt dem Zertifikatsantrag für den öffentlichen Validierungsschlüssel beigefügt und durch die Zertifizierungsstelle im Zertifikat für den öffentlichen Validierungsschlüssel als zusätzliches Attribut inkludiert. Das Zertifikat ist damit in eindeutiger Weise mit dem signierten elektronischen Dokument verknüpft.

Anstelle einer Nutzung eines zentralen Hardware-Sicherheitsmoduls ist auch eine Nutzung eines persönlichen Sicherheitsmoduls zur Signaturerzeugung möglich. Dabei wird der Hash-Wert für das zu signierende elektronische Dokument beispielsweise an einem Personal Computer o.ä. erzeugt und über eine Infrarot- oder Bluetooth-Schnittstelle an das persönliche Sicherheitsmodul übermittelt.

Eine weitere Anwendung des erfindungsgemäßen Signaturverfahrens besteht in einer Nutzung eines modifizierten und mit einer Validierungslogik versehenen Druckers. Als Eingangsparameter erhält ein solcher Validierungsdrucker ein zu signierendes elektronisches Dokument und eine für dieses elektroni-

sche Dokument berechnete elektronische Signatur. Bei erfolgreicher Validierung der elektronischen Signatur wird das zugehörige elektronische Dokument auf dem Validierungsdrucker ausgegeben. Anschließend wird dem Verfasser des elektronischen Dokuments die Möglichkeit geboten anhand des Ausdrucks zu entscheiden, ob er den zuvor verwendeten privaten Signaturschlüssel zertifizieren lassen will.

Die Anwendung der vorliegenden Erfindung ist nicht auf die hier beschriebenen Ausführungsbeispiele beschränkt.

Patentansprüche

1. Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen, bei dem
- ein asymmetrisches Schlüsselpaar erzeugt wird, das einen privaten Signaturschlüssel und einen öffentlichen Validierungsschlüssel umfaßt,
- zumindest eine elektronische Signatur mittels des privaten Signaturschlüssels und durch Anwendung einer vorgebbaren Signaturfunktion für zumindest ein elektronisches Dokument berechnet wird,
- nach Berechnung der zumindest einen elektronischen Signatur eine Zertifizierung des öffentlichen Validierungsschlüssels erfolgt.

2. Verfahren nach Anspruch 1, bei dem
bei einer Validierung nur Signaturen als gültig erkannt werden, die zu einem Zeitpunkt vor der Zertifizierung des öffentlichen Validierungsschlüssels erzeugt werden und/oder wurden.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem
bei der Zertifizierung des öffentlichen Validierungsschlüssels zusätzlich zu einem Benutzeridentifikator und dem öffentlichem Validierungsschlüssel zumindest eine Referenz auf das zumindest eine elektronische Dokument einbezogen wird.

4. Verfahren nach Anspruch 3, bei dem
eine Implementierung der zumindest einen Referenz durch eine Berechnung eines Hash-Wertes für das zumindest eine elektronische Dokument erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, bei dem
nach Berechnung der Signatur und vor deren Übermittlung an einen Empfänger eine Validierung durch einen Verfasser des zumindest einen elektronischen Dokuments zur Überprüfung ei-

ner durch das zumindest eine elektronische Dokument ausgedrückten Willenshandlung erfolgt.

FIG 1 Stand der Technik

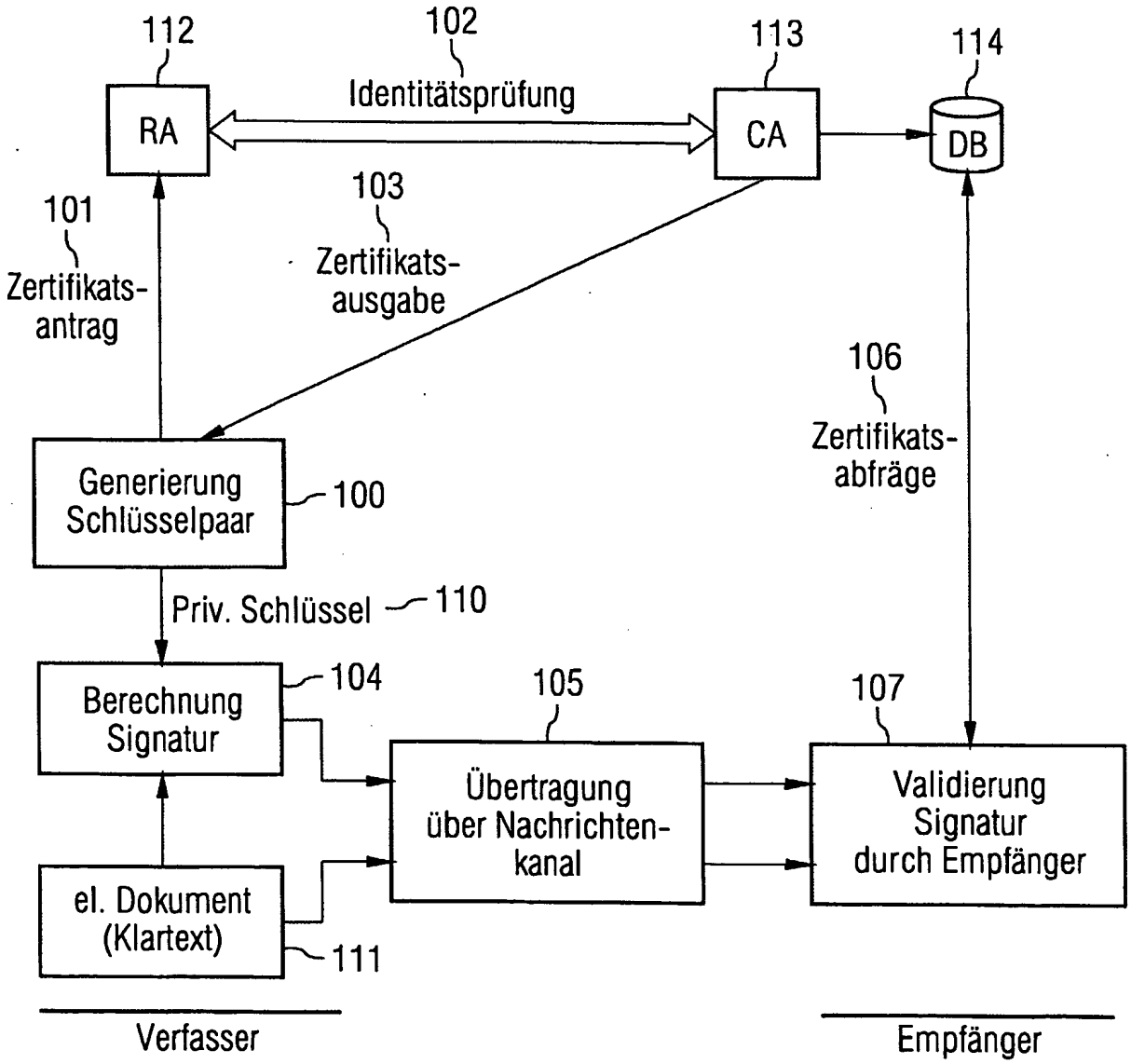
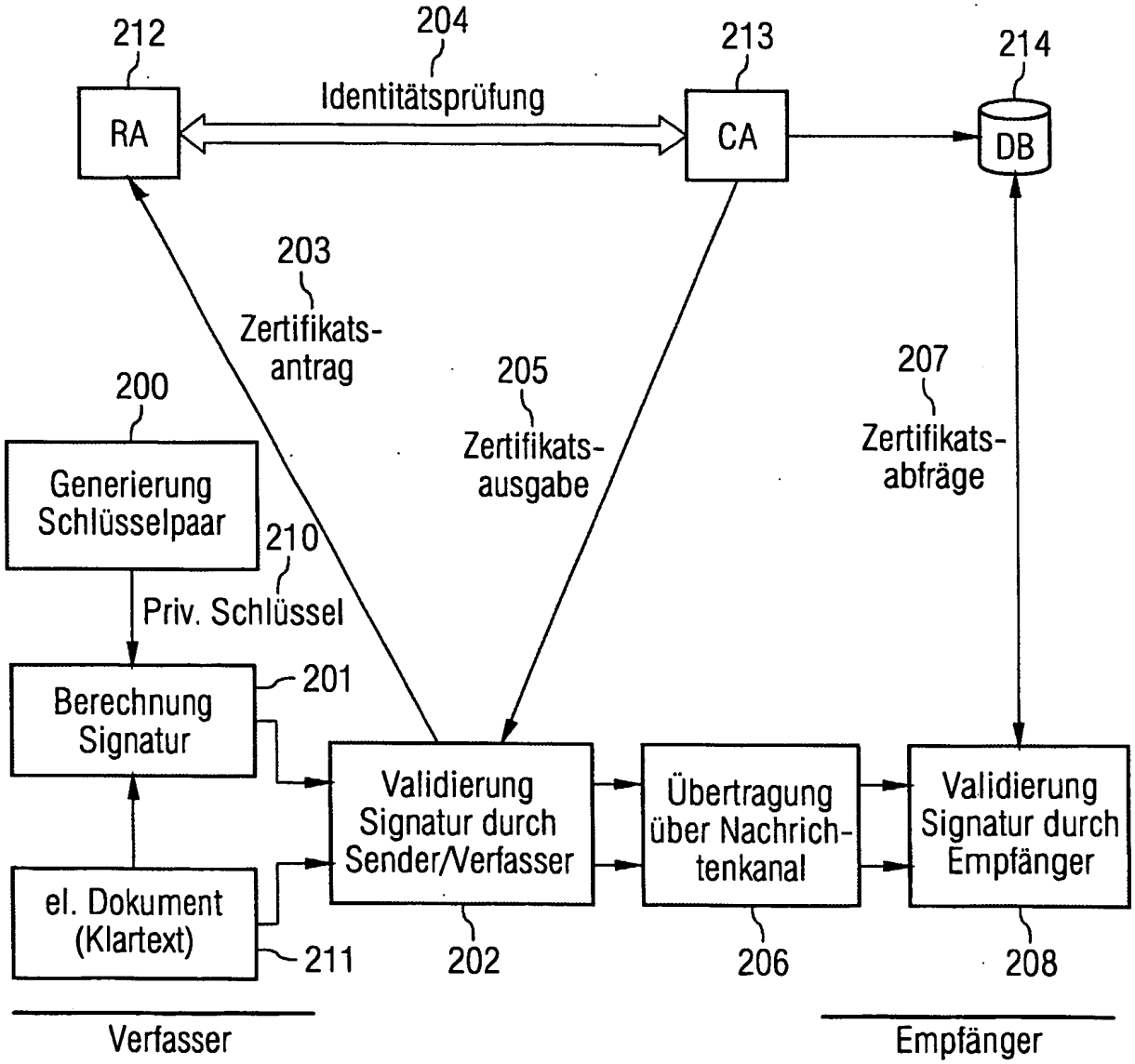


FIG 2


212
204
213
214
RA
Identitätsprüfung
CA
DB
203
Zertifikats-
antrag
205
Zertifikats-
ausgabe
207
Zertifikats-
abfräge
200
Generierung
Schlüsselpaar
210
Priv. Schlüssel
Berechnung
Signatur
201
Validierung
Signatur durch
Sender/Verfasser
Übertragung
über Nachrich-
tenkanal
Validierung
Signatur durch
Empfänger
el. Dokument
(Klartext)
211
202
206
208
Verfasser
Empfänger

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/10327

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 373 561 A (HABER STUART A ET AL) 13 December 1994 (1994-12-13) column 1, line 10 - line 15 column 3, line 22 -column 4, line 23	1-5
A	US 5 208 858 A (VOLLERT EMMERAN ET AL) 4 May 1993 (1993-05-04) abstract column 1, line 14 - line 39 column 3, line 68 -column 4, line 50	1-5
A	EP 1 191 743 A (CERTICOM CORP) 27 March 2002 (2002-03-27) abstract	1-5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 November 2003	05/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/10327

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5373561 A	13-12-1994	AU 670166 B2	04-07-1996
		AU 5670694 A	19-07-1994
		CA 2151590 A1	07-07-1994
		DE 69333068 D1	31-07-2003
		EP 0676109 A1	11-10-1995
		JP 8504965 T	28-05-1996
		WO 9415421 A1	07-07-1994
US 5208858 A	04-05-1993	DE 4003386 C1	23-05-1991
		AT 129369 T	15-11-1995
		DE 59009799 D1	23-11-1995
		EP 0440914 A2	14-08-1991
		ES 2077621 T3	01-12-1995
EP 1191743 A	27-03-2002	CA 2357792 A1	20-03-2002
		EP 1191743 A2	27-03-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 03/10327

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 373 561 A (HABER STUART A ET AL) 13. Dezember 1994 (1994-12-13) Spalte 1, Zeile 10 - Zeile 15 Spalte 3, Zeile 22 -Spalte 4, Zeile 23	1-5
A	US 5 208 858 A (VOLLERT EMMERAN ET AL) 4. Mai 1993 (1993-05-04) Zusammenfassung Spalte 1, Zeile 14 - Zeile 39 Spalte 3, Zeile 68 -Spalte 4, Zeile 50	1-5
A	EP 1 191 743 A (CERTICOM CORP) 27. März 2002 (2002-03-27) Zusammenfassung	1-5

☐ *Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen*

☒ *Siehe Anhang Patentfamilie*

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. November 2003	05/12/2003

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Post, K

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 03/10327

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5373561	A	13-12-1994	AU	670166 B2	04-07-1996
			AU	5670694 A	19-07-1994
			CA	2151590 A1	07-07-1994
			DE	69333068 D1	31-07-2003
			EP	0676109 A1	11-10-1995
			JP	8504965 T	28-05-1996
			WO	9415421 A1	07-07-1994
US 5208858	A	04-05-1993	DE	4003386 C1	23-05-1991
			AT	129369 T	15-11-1995
			DE	59009799 D1	23-11-1995
			EP	0440914 A2	14-08-1991
			ES	2077621 T3	01-12-1995
EP 1191743	A	27-03-2002	CA	2357792 A1	20-03-2002
			EP	1191743 A2	27-03-2002